UNIVERSITÀ DEGLI STUDI DI PADOVA
Tesi di Laurea Magistrale

UNIVERSITÉ DE BORDEAUX
Mémoire de Master 2

THE NÉRON-OGG-SHAFAREVICH CRITERION

Pietro GATTI

Advisor: Nicola MAZZARI

July 2014

Contents

Introduction

As Ogg has shown in [12] the good reduction of an elliptic curve can be seen by the non-ramification of its torsion groups; apparently this result was also known to Shafarevich. In [15] Serre and Tate generalized this criterion to the case of abelian varieties, naming it after Néron, Ogg and Shafarevich. This is due to the fact that the fundamental tool they used to generalize the result to abelian varieties are the Néron models, introduced by André Néron in [11]. The Néron-Ogg-Shafarevich criterion can be stated as follows.

Theorem. *Let K be a field with a discrete valutation v such that its residue field k is perfect. Let A be an abelian variety over K and l a prime number different from the characteristic of k. Then the following are equivalent:*

(a) A has good reduction at v;

(b) $A[m]$ is unramified at v for every integer m coprime to $\mathrm{char}(k)$*;*

(c) $A[m]$ is unramified at v for infinitely many integers m coprime to $\mathrm{char}(k)$*;*

(d) $T_l(A)$ is unramified at v.

The proof of this result essentially consists of two lemmas. One of them is due to some decomposition results for group varieties, while the other comes from the fact that the maximal unramified extension of K has a Henselian ring of integers. By mean of the theory of Néron models the proof of the second lemma reduces to an application of Hensel's lemma.

The aim of this thesis is to present the proof of this theorem following the guideline provided by [15]. Our intention is not only to provide the reader with all the theory needed to appreciate the statement, but moreover to give more details on the original proof in order to make it clearer to an unexpert mathematician who faces the original article (for example a master student in mathematics). The theory we expose as the needed background to understand the Néron-Ogg-Shafarevich criterion has not only the proof of this result as a final goal. In fact the theorem can be seen as an opportunity to give an exhaustive, within a certain level, exposition of some topics in arithmetic. Of course the fact that we wanted to prove a certain statement influenced our choices. As a consequence of this, the reader should observe that some canonical results are presented in a slightly more general context to fit in the hypothesis of the theorem. For example one can appreciate that we developed the theory of abelian varieties over a non-algebraically closed field (while this is not the case in [10]) or that we gave the basic notions for ramification theory in the case of an infinite extension without assuming the base field to be complete. For what concerns the language, the best environment to set this work turned out to be the group schemes, the theory of abelian varieties and the claimed decompostion results are presented in these terms. We are going to use definitions in scheme theory without recalling them: we refer to [7] for the common langauge, unless otherwise stated. The basic results in algebraic geometry are not stated but we tried to give a reference to them even when using the most basic ones.

The content of this work is divided in three chapters. The first one consists of preliminaries, for algebraic geometry we set the basic definitions and properties of group schemes providing some examples. For what concerns number theory we describe ramification in the infinite extension case. In the second chapter we will talk about abelian varieties, after having defined them we will describe some of their properties. Here we will define Tate modules and the Galois action on them. Aside from this we will consider the issue of good reduction, and so we will introduce abelian schemes and Néron models. The topic of the last chapter is the proof of the Néron-Ogg-Shafarevich criterion. The first part is essentially devoted to some decomposition of group schemes that will allow us to prove a lemma needed for the second part. In the second section we present the proof of the announced criterion for good reduction of abelian varieties.

Chapter 1

Preliminaries

In this chapter we will set the background needed in algebraic geometry with group schemes and in number theory with theory of ramification.

1.1 Group schemes

Group schemes are group objects in the category of schemes. In other words they are schemes with morphisms that make them behave as groups. In this section, starting from this definition, we will see that group schemes also have an equivalent functorial behaviour. We will conclude this introductive section with some examples.

Definition 1.1.1. Let S be a scheme. A *group scheme over S* (or an *S-group scheme*) is a scheme G over S, given by $\pi : G \to S$, together with S-morphisms

$$\begin{aligned} m &: G \times_S G \longrightarrow G && \text{(multiplication)} \\ e &: S \longrightarrow G && \text{(identity)} \\ i &: G \longrightarrow G && \text{(inverse)} \end{aligned}$$

such that the following diagrams are commutative

$$\begin{tikzcd}
G \times_S G \times_S G \arrow[r, "m\times \mathrm{id}_G"] \arrow[d, "\mathrm{id}_G \times m"'] & G \times_S G \arrow[d, "m"] \\
G \times_S G \arrow[r, "m"'] & G
\end{tikzcd}$$

$$\begin{tikzcd}
S \times_S G \arrow[rr, "e\times \mathrm{id}_G"] \arrow[dr, "j_1"'] & & G \times_S G \arrow[dl, "m"] \\
& G &
\end{tikzcd}
\qquad
\begin{tikzcd}
G \times_S S \arrow[rr, "\mathrm{id}_G \times e"] \arrow[dr, "j_2"'] & & G \times_S G \arrow[dl, "m"] \\
& G &
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[d, "(\mathrm{id}_G{,}i)"'] & S \arrow[d, "e"] \\
G \times_S G \arrow[r, "m"] & G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[d, "(i{,}\mathrm{id}_G)"'] & S \arrow[d, "e"] \\
G \times_S G \arrow[r, "m"] & G
\end{tikzcd}$$

where j_1 and j_2 are the canonical isomorphisms.

Definition 1.1.2. A group scheme over S is said *commutative* if the following diagram commutes

$$\begin{tikzcd}
G \times_S G \arrow[r, "m"] \arrow[d, "s"'] & G \arrow[d, "\mathrm{id}_G"] \\
G \times_S G \arrow[r, "m"] & G
\end{tikzcd}$$

where s is the "switch" morphism that exchanges the two factors of the fiber product.

Definition 1.1.3. Let (G, m, e, i) be a group scheme over S. Then a subscheme $j : H \hookrightarrow G$ is a *subgroup scheme* of G if there exist S-morphisms m_H, e_H, i_H such that

$$\begin{aligned} m \circ (j \times j) &= j \circ m_H \\ e &= e_H \circ j \\ j \circ i &= i_h \circ j \end{aligned}$$

Remark 1. One can define *normal subgroup schemes* defining properly a conjugation action as an S-morphism from $G \times_S G \times_S G$ to G. Then we say that a subgroup scheme H is normal if the conjugation factors through H. The details of the construction of this map are cumbersome. Later we will give an equivalent definition that is simpler to handle.

Definition 1.1.4. Let (G_1, m_1, e_1, i_1) and (G_2, m_2, e_2, i_2) be two group schemes over S. A *homomorphism of group schemes over* S from G_1 to G_2 is an S-morphism $f : G_1 \to G_2$ such that

$$f \circ m_1 = m_2 \circ (f \times f).$$

This automatically implies

$$\begin{aligned} f \circ e_1 &= e_2 \\ f \circ i_1 &= i_2. \end{aligned}$$

When no confusion will be possible we will refer to an S-group scheme (G, m, e, i) just by G.

For any integer n, we denote by $[n] : G \to G$ the *n-power* morphism (*n-multiple* in the commutative case). It is given by

$$[n] = (G \xrightarrow{\Delta_G^n} G^n \xrightarrow{m^n} G)$$

where Δ_G^n is the n-diagonal morphism and m^n is the n-th iterate of the multiplication by m.

Other interesting S-morphisms coming from the group scheme structure are the translations. To define them we bserve that for every S-scheme T, the base change $G_T := G \times_S T$ naturally inherits a structure of group scheme over T (if G is commutative, then G_T is commutative). In this situation we give this definition.

Definition 1.1.5. For any T-rational point x in $G(T)$, we define the *right translation* $t_x : G_T \to G_T$ and the *left translation* ${}_xt : G_T \to G_T$, as the T-morphisms given by the compositions

$$t_x = (G_T \simeq G_T \times_T T \xrightarrow{\mathrm{id}_{G_T} \times x} G_T \times_T G_T \xrightarrow{\quad m \quad} G_T)$$

and

$${}_xt = (G_T \simeq T \times_T G_T \xrightarrow{x \times \mathrm{id}_{G_T}} G_T \times_T G_T \xrightarrow{\quad m \quad} G_T)\ .$$

Then t_x is an isomorphism being $t_{i(x)}$ its right and left inverse. Of course, the same is true for ${}_xt$.

It is easy to show that every S-group scheme G can be seen as a functor from $\mathbf{Sch}_S$ to $\mathbf{Grp}$. In fact let T be a scheme over S with structure morphism $\pi_T : T \to S$, then $G(T)$, the set of T-rational points of G, is a group: the multiplication of two T-rational points x and y is given by $x * y = m \circ (x, y)$, the identity element is $e \circ \pi_T$, the inverse is given by $x^{-1} = i \circ x$. Functoriality is just an easy check.
Now we will show a sort of converse to this construction, that is a way to associate to a functor of this kind a group scheme. To do this we introduce some easy notions of category theory.
Let $\mathcal{C}$ be a category, we denote with $\hat{\mathcal{C}}$ the category of contravariant functors from $\mathcal{C}$ to $\mathbf{Set}$, whose morphisms are natural transformations of contravariant functors. So, for example, given an object C in $\mathcal{C}$ we have a contravariant functor $h_C = \mathrm{Hom}_{\mathcal{C}}(-, C)$ which is an object in $\hat{\mathcal{C}}$. This kind of contravariant functors are particularly important because of the following result.

Lemma 1.1.6 (Yoneda Lemma)**.** *The functor $h : \mathcal{C} \to \hat{\mathcal{C}}$, associating to $C \in \mathcal{C}$ the contravariant functor h_C, is fully faithful. Moreover for every $C \in \mathcal{C}$ and for every $F \in \hat{\mathcal{C}}$, we have a canonical bijection $F(C) \to \mathrm{Hom}_{\hat{\mathcal{C}}}(h_C, F)$.*

By this we can deduce the following.

Proposition 1.1.7. *Let G be a scheme over S. Then the data of a group scheme structure on G (in the sense of definition 1.1.1) is equivalent to the data of a representable contravariant functor from $\mathbf{Sch}_S$ to $\mathbf{Grp}$, together with the choice of G as a representing object.*

Proof. We already showed that $G(-) = \mathrm{Hom}_S(-, G) : \mathbf{Sch}_S \to \mathbf{Grp}$ is a contravariant functor.
Conversely we assume that the functor $h_G = \mathrm{Hom}_S(-, G) : \mathbf{Sch}_S \to \mathbf{Set}$ can be lifted to a functor $\tilde{h}_G : \mathbf{Sch}_S \to \mathbf{Grp}$. So for every S-scheme T we have a multiplication map

$$m_T : h_G(T) \times h_G(T) \to h_G(T).$$

Since $h_{G \times_S G}$ and $h_G \times h_G$ are naturally isomorphic, the maps m_T's induce a natural transformation of functors

$$\mu : h_{G \times_S G} \to h_G.$$

So μ is a morphism in the category $\hat{\mathbf{Sch}}_S$ and so by Yoneda's lemma, we can associate to μ an S-morphism $m : G \times_S G \to G$.

Exactly in the same way, one can build the morphisms e and i. Then using the group structure on $h_G(T)$ for every T, one can prove that the morphisms m, e and i satisfy the properties in definition 1.1.1. □

Given a functor h_G, with abuse of notation, we will refer also to its group-valued lifting as h_G.

Remark 2. Following what proved just before one can easily show that:

1. Saying that H is a subgroup scheme of an S-group scheme G is equivalent to saying that h_H is a subgroup functor of h_G, meaning that $h_H(T)$ is a subgroup of $h_G(T)$ for every S-scheme T.
2. The data of an S-group scheme morphism $f : G_1 \to G_2$ (in the sense of the definition 1.1.4) is equivalent to the data of a natural transformation of group-valued functors $h_{G_1} \to h_{G_2}$.

Remark 3. What is actually holding is an equivalence of categories between the category of group schemes over S and the category of representable functors from $\mathbf{Sch}_S$ to $\mathbf{Grp}$. This now can be easily verified.

In view of this, we will naturally confuse a group scheme G with its associated group-valued functor h_G.
This correspondence will allows us to define simply what a *normal subgroup scheme* is.

Definition 1.1.8. Let G be a group scheme over S and H a subgroup scheme of G. We will say that H is a *normal subgroup scheme* of G is $h_H(T)$ is a normal subgroup of $h_G(T)$ for every S-scheme T.

The equivalent definitions of group schemes make easier to understand the following examples.

Example 1. To every S-scheme T, we can associate the additive group of the global section of T, namely $\Gamma(T, \mathcal{O}_T)$. This gives us a group scheme over S, which is called the *additive group* over S and is denoted by $\mathbb{G}_{a,S}$.
If $S = \mathrm{Spec}(R)$ is affine, then $\mathbb{G}_{a,S}$ is represented by the affine scheme $\mathbb{A}^1_S = \mathrm{Spec}(R[x])$, the group scheme structure morphisms are induced by the ring morphisms

$$\tilde{m} : x \mapsto x \otimes 1 + 1 \otimes x$$
$$\tilde{e} : x \mapsto 0$$
$$\tilde{i} : x \mapsto -x$$

Example 2. To every S-scheme T, we can associate the multiplicative group of the invertible elements of the global section of T, namely $\Gamma(T, \mathcal{O}_T)^{\times}$. This gives us a group scheme over S, which is called the *multiplicative group* over S and is denoted by $\mathbb{G}_{m,S}$.
If $S = \mathrm{Spec}(R)$ is affine, then $\mathbb{G}_{m,S}$ is represented by the affine scheme $\mathrm{Spec}(R[x, x^{-1}])$

(this is the affine punctured line), the group scheme structure morphisms are induced by the ring morphisms

$$\begin{gathered}\tilde{m} : x \mapsto x \otimes x\\ \tilde{e} : x \mapsto 1\\ \tilde{i} : x \mapsto x^{-1}\end{gathered}$$

Example 3. Let Γ be a group. Then we consider the S-scheme $G := \coprod_{\gamma\in\Gamma} S$. This is naturally a group scheme, in fact it is sufficient to observe that $G \times_S G$ is isomorphic to $\coprod_{\gamma,\gamma'\in\Gamma}$. Then the multiplication map is given by the morphism that maps identically the component of $G \times_S G$ indexed by (γ, γ') to the component of G indexed by $\gamma\gamma'$. In the same way the identity section is the morphism sending S identically to the component of G indexed by e_Γ, the inverse morphism maps identically the component indexed by γ to the component indexed by γ^{-1}. This group scheme is called the *constant group over S with fiber* Γ and it is usually denoted by $G = \Gamma_S$.

We want now to understand how G acts functorially on an S-scheme T. Since the group structure on $G(T)$ is induced by composition with $T \to G$, we observe that given an S-morphism $T \to G$, the only thing that matters for the group law is which are the indeces of G in which the image of T is contained. In this way it appears clear that, as groups, we have an isomorphism between $G(T)$ and the group of locally constant functions from T to Γ.

We want to remark that if $\mathbb{Z}_S$ is the constant group with fiber $\mathbb{Z}$ we have

$$\mathrm{Hom}_{\mathbf{GrpSch}_S}(\mathbb{Z}_S, G) = \mathrm{Hom}_{\mathbf{Sch}_S}(S, G) = G(S).$$

In fact a group scheme morphism $\mathbb{Z}_S \to G$ is univocally determined by a morphism $S \to G$ on the copy of S in $\mathbb{Z}_S$ indexed by 1.

1.2 Ramification theory

The aim of this section is to extend the concept of *ramification* for finite extensions of discrete valued field, to ramification of the action of the absolute Galois group. Here we are recalling some facts about finite extensions of discrete valuation fields. Most of them will be useful to understand the infinite case we will describe later, some of them are proposed mainly for cultural reasons. The main reference for what stated without a proof is [14, I, §4].

Throughout this section K will be a field with a discrete valuation v, we will denote by $\mathcal{O}_v$ its *ring of integers*, that is the subring of elements with non-negative valuation. This one is a local ring and we will denote by $\mathfrak{m}_v$ its unique maximal ideal (it is given by the elements with positive valuation). The *residue field* of the valuation v will be $k := \mathcal{O}_v/\mathfrak{m}_v$. We will always assume k to be perfect.[1]

We consider now a finite extension K'/K, with degree $[K' : K] = n$.

Proposition 1.2.1. *There exists at least one discrete valuation v' on K' such that $v' |_K = v$.*

[1] Even though this assumption may be too restrictive for some results proposed in this chapter, it will be crucial in the last one. This is why we put it here.

In light of the proposition the ring $\mathcal{O}_{v'}$ will be the ring of integers of v', its maximal ideal will be $\mathfrak{m}'_v$ and k' will be its residue field.
We recall that to an extension of discrete valuation of this kind we can associate two positive integers:

$$e(v'/v) := |v'(K') : v(K)|$$

called the *ramification index* of v' at v; and

$$f(v'/v) := [k' : k]$$

called the *residue degree* of v in the extension K'/K. Moreover we have that $e(v'/v)$ and $f(v'/v)$ do not depend on the choice of v'. Assume that v'' is another extension of v, the Galois group acts transitively on the set of prime ideals over a given ideal and so by unique factorization of ideals in Dedekind domains, we have that $e(v''/v) = e(v'/v)$. Moreover the transitivity of the action give us an isomorphism between k'' and k', establishing $f(v''/v) = f(v'/v)$. For details see [14, Ch. I, §7, Prop. 19 & Cor.]. So, when the galois field extension will be understood, we will simply denote with e and f the ramification index and the residue degree respectively.
Under some further assumptions (i.e. K is complete, K'/K is separable, ...) we have the following relation.

Proposition 1.2.2.

$$n = ef$$

For our purposes we will give the following definition.

Definition 1.2.3. The extension K'/K is said to be *unramified* at v if $e(v'/v)$ is equal to 1.

We now assume K'/K to be a Galois extension with Galois group $\mathrm{Gal}(K'/K)$. It is easy to check that, then, the finite extension k'/k is Galois.
We denote by $S_v(K')$ the set of equivalence classes of discrete valuations on K' extending v. Then $\mathrm{Gal}(K'/K)$ acts on $S_v(K')$ by $\sigma[w] = [w \circ \sigma]$.
In this context we give the following definitions.

Definition 1.2.4. The *decomposition group* of v' is the subgroup of $\mathrm{Gal}(K'/K)$ that fixes the class of v'. Namely it is

$$D_{K'/K}(v') := \{\sigma \in \mathrm{Gal}(K'/K) \mid \sigma[v'] = [v' \circ \sigma] = [v']\}$$

Definition 1.2.5. The *inertia group* of v' is the subgroup of $\mathrm{Gal}(K'/K)$ given by

$$I_{K'/K}(v') := \{\sigma \in \mathrm{Gal}(K'/K) \mid v'(\sigma(a) - a) > 0, \forall a \in \mathcal{O}_{v'}\}$$

To ease the notation, we will write D and I for the decomposition group and the inertia group respectively. It is easy to check that D and I are actually subgroups of $\mathrm{Gal}(K'/K)$. Moreover I is a normal subgroup of D.
One sees that the Galois action on K' can be restricted to an action on $\mathcal{O}_{v'}$. This naturally induces, by reduction, an action of D on k'. More explicitly, we have the following statement.

Proposition 1.2.6. *The reduction map*

$$r : D \to \mathrm{Gal}(k'/k)$$

is a surjective homomorphism, with kernel I.

Proof. See [14, I, §7, Prop. 20] and [14, IV, §1, Lemma 1]. □

We introduced the inertia group because this allows us to characterize unramified extensions.

Proposition 1.2.7. *A subextension L of K' over K (with discrete valuation induced by restriction of v') is unramified at v, if and only if I acts trivially on L.*

Proof. As one can see in [14, IV, §1, Cor. 2] the subfield of K' fixed by I, is the maximal unramified subextension of K' over K. This is enough to conclude. □

Now we are going to extend this concept to infinite extensions. We recall that an algebraic field extension Ω/K (possibly infinite) is said to be *Galois* if it is normal and separable. Its Galois group is given by

$$\mathrm{Gal}(\Omega/K) := \varprojlim \mathrm{Gal}(F/K)$$

where F ranges through the finite Galois extensions of K contained in Ω. This is a topological group, with the profinite topology (for details see [13, Ch.2 §11]). We recall that there is a Galois correspondence between closed subgroups $H \subset \mathrm{Gal}(\Omega/K)$ and intermediate extensions $K \subset L \subset \Omega$:

$$\begin{aligned} H &\longmapsto E(H) := \{x \in K_s \mid \sigma(x) = x, \forall \sigma \in \Omega\} \\ L &\longmapsto \mathrm{Gal}(\Omega, L) := \{\sigma \in \mathrm{Gal}(\Omega/K) \mid \sigma(x) = x, \forall x \in L\}. \end{aligned}$$

For details see [13, Th. 2.11.3]. We denote by K_s a separable closure of K. This is the subfield of a fixed algebraic closure of K given by all the elements separable over K.

Proposition 1.2.8. *The field K_s is normal and separable, hence Galois, over K.*

Proof. We know that K_s is separable over K by definition. Moreover every minimal polynomial of an element in K_s over K is separable, hence it factors completely in K_s, so K_s is normal. □

By the proposition, K_s is a maximal Galois extension of K, this justifies calling $\mathrm{Gal}(K_s/K)$ the *absolute Galois group* of K.
We now assume the field K to be endowed with a discrete valuation v, with $\mathcal{O}_v$ as its ring of integers and k as its residue field, again we assume k to be perfect. For every finite Galois extension F/K we can define on F a discrete valuation v_F extending v. We can require, moreover, these discrete valuations to be compatible with respect to restrictions. That is, for every two finite Galois extensions F', F'', we have $v_{F'}$ and $v_{F''}$ agree on $F' \cap F''$. By a direct limit argument we can extend this compatible system of discrete valuations to a valuation $\bar{v}$ on K_s.

Remark 4. The valuation $\bar{v}$ is not discrete. In fact, let π be a uniformizer of v in $\mathcal{O}_v$. Then for every positive integer m coprime with $\mathrm{char}(K)$, there is an element α_m in K_s such that $\alpha_m^m = \pi$, this implies that $\bar{v}(\alpha_m) = 1/m$.

As in the discrete case we have the following notations.

$$\mathcal{O}_{\bar{v}} := \{a \in K_s \mid \bar{v}(a) \geq 0\}$$

is a subring of K_s, it is a valuation ring hence local and integrally closed. The ideal

$$\mathfrak{m}_{\bar{v}} := \{a \in K_s \mid \bar{v}(a) > 0\}$$

corresponds to the only maximal ideal of $\mathcal{O}_{\bar{v}}$. The *residue field* of the extension K_s/K will be $\bar{k} := \mathcal{O}_{\bar{v}}/\mathfrak{m}_{\bar{v}}$.

Remark 5. The "bar" in the symbol for the residue field is not misleading. In fact one can easily prove that $\mathcal{O}_{\bar{v}}/\mathfrak{m}_{\bar{v}}$ is an algebraic closure of k.

The following definition naturally arises.

Definition 1.2.9. We will call the *inertia group* of $\bar{v}$ the subgroup of $\mathrm{Gal}(K_s/K)$ given by

$$I(\bar{v}) = \varprojlim I_{F/K}(v_F)$$

with F running through the finite Galois extensions of K.

We will denote, since there is no possible confusion, $I = I(\bar{v})$. From the definition it is immediate that

$$I = \{\sigma \in \mathrm{Gal}(K_s/K) \mid \bar{v}(\sigma(a) - a) > 0, \forall a \in \mathcal{O}_{\bar{v}}\}.$$

Moreover I is a closed subgroup (see [13, Cor. 1.1.8(b)]), hence by Galois correspondence $K_s^I = E(I)$, the set of elements of K_s fixed by the action of I, is a field. We will denote $L = K_s^I$.

Proposition 1.2.10. *The field L is the maximal unramified extension of K.*

Proof. By definition $I = \varprojlim I_{F/K}(v_F)$, with F/K finite Galois extensions. Applying $E(-)$ to both sides we have

$$L = E(I) = E(\varprojlim I_{F/K}(v_F)) = \varinjlim E(I_{F/K}(v_F)).$$

As seen in proposition 1.2.7 the fields $E(I_{F/K}(v_F))$ are unramified at v. Moreover every unramified extension K'/K is contained in an unramified finite Galois extension F/K. Hence $E(I)$ is the compositum of all unramified extensions of K. □

This allows us to define unramified extensions in the following way that coincides with the standard definition for finite extensions.

Definition 1.2.11. A subfield of K_s containing K is *unramified* at v if I acts trivially on it.

By restriction, the field L is a valuation field whose valuation ring is $\mathcal{O}_L := \mathcal{O}_{\bar{v}} \cap L$. This has only one maximal ideal $\mathfrak{m}_L := \mathfrak{m}_{\bar{v}} \cap L$. Moreover we have the following result that will be useful in the last chapter.

Lemma 1.2.12. *The ring $\mathcal{O}_L$ is Henselian (it satisfies Hensel's Lemma).*

Proof. Let $f \in \mathcal{O}_L[x]$ be a monic irreducible polynomial, we denote by $\bar{f}$ the reduction modulo $\mathfrak{m}_L$ of f. Let us suppose that $\bar{f}$ has a simple root a modulo $\mathfrak{m}_L$, that is

$$\bar{f}'(a) \not\equiv 0 \pmod{\mathfrak{m}_L}$$

This means that $f' \in \mathcal{O}_L[x]$ is not zero and so f is separable, implying that it has all its roots in K_s. Since f is monic with coefficients in $\mathcal{O}_{\bar{v}}$, that is integrally closed, all the roots of f are $\bar{v}$-integers. Since f and $\bar{f}$ have the same degree, all the roots of $\bar{f}$ (with multiplicities) are obtained bijectively from reduction of roots of f modulo $\mathfrak{m}_{\bar{v}}$. So there is α in $\mathcal{O}_{\bar{v}}$ that reduces to a. Now let σ be an element of I, then $\sigma(\alpha)$ is a root of f, since both $\sigma(\alpha)$ and α reduce to a modulo $\mathfrak{m}_{\bar{v}}$, they are forced to be equal. Then $\sigma(\alpha) = \alpha$ for every σ in I, and so α is in $\mathcal{O}_L$ as required. □

Chapter 2

Abelian varieties

2.1 Definition and properties

In this section K will be a field and we use the following definitions.

Definition 2.1.1. Let X be a scheme over K. We say that X is a *variety* if X is separated, of finite type and geometrically integral. A *morphism of varieties* is a morphism of K-schemes between varieties. We will say that a variety is *complete* if it is proper as a scheme.

Definition 2.1.2. A variety G over K that is a group scheme over K, is called a *group variety.*

Actually the separatedness of a group variety coul be not required in the definition, in fact, as the following lemma shows, it holds for every group scheme over a field.

Lemma 2.1.3. *Let G be a group scheme over a field K, then G is separated.*

Proof. It is enough to prove that $\Delta(G)$ is closed in $G \times_K G$ (see [7, Ch. 3, Cor. 3.5]). Then we consider the diagram

$$\begin{tikzcd}
G \times_K G \arrow[r, "d_G"] & G \\
G \arrow[u, "\Delta"] \arrow[r] & \mathrm{Spec}(K) \arrow[u, "e_G"']
\end{tikzcd}$$

where $d_G = m_G \circ (id_G \times i_G)$ is the difference morphism. Then $\Delta(G)$ is exactly the preimage by d of the image of e, since e is a closed map and d is continuous, we have the desired result. □

A nice use of the group structure on a group variety is shown in the following proposition.

Proposition 2.1.4. *Group varieties are smooth.*

Proof. Let G be a group variety over K. By definition X is smooth if and only if $X_{\bar{K}}$ is regular. By [7, Ch. 4, Cor. 2.17] it is enough to check that every closed point of $X_{\bar{K}}$ is regular, moreover we know that the closed points of $X_{\bar{K}}$ are exactly the points in $X_{\bar{K}}(\bar{K})$ ([3, Cor. 6.4.3]). So we are reduced to show that every x in $X_{\bar{K}}(\bar{K})$ is regular. Let x_0 in $X_{\bar{K}}(\bar{K})$ be a regular point (it exists because of [7, Ch. 4, Lemma 2.21]). For every closed point x, we have a closed point $x_0 - x$, given by the group-law on $X_{\bar{K}}(\bar{K})$. Then we consider the translation $t_{x_0-x} : X_{\bar{K}} \to X_{\bar{K}}$. This is an isomorphism of schemes sending x to x_0, since the last one is regular, also x will be regular. □

Among group varieties we focus our attention on the complete ones.

Definition 2.1.5. An *abelian variety* over K is a complete group variety over K.

The theory of abelian varieties is really wide and there are entire books dedicated to them, what we want to provide here is just a brief collection of properties that we will use later. Even though a canonical reference for the subject is [10], for our aims we do not require K to be algebraically closed. So in most of the cases we will refer to [18].
We want to show that requiring two varieties to be abelian strongly reduces the possible morphisms of varieties between them. In a certain sense the subcategory **AbVar** ⊂ **Var** is "not so far" from being full, in fact for two abelian varieties A and B, the set $\mathrm{Hom}_{\mathbf{Var}}(A, B)$ can be described in terms of $\mathrm{Hom}_{\mathbf{AbVar}}(A, B)$. To give a first idea of how this is proved we imagine the following easy situation.
We have two groups A and B, and a function between them $f : A \to B$. One may ask whether f is a homomorphism. Obviuosly there are functions that are not homomorphisms, for instance every function such that $f(e_A) \neq e_B$. But it may happen that f is just a translation of a homomorphism h by an element y in B. Explicitly $f(x) = h(x)+y$, for every x in A. Of course there are functions that do not satisfy this condition, but showing a procedure to check if this holds, we will give the idea of the proof of the following proposition. Obviously the first requirement is that $y = f(e_A)$, then we have to check that $h(\cdot) = f(\cdot) - y$ is a group homomorphism. To do this we can build the function

$$\begin{aligned} g : A \times A &\longrightarrow B \\ (x, x') &\longmapsto h(x + x') - h(x') - h(x) \end{aligned}$$

then h is a homomorphism if and only if g is constantly e_B. It is clear that this cannot hold for every function f, on the other hand this is what is happening for abelian varieties, and this is due to the fact that we asked them to be complete.

Proposition 2.1.6. *Let A and B be two abelian varieties, then a morphism of varieties $f : A \to B$ is given by $f = t_y \circ h$, where t_y is the translation by a point y in B and h is a morphism of group schemes.*

Proof. We will reproduce the argument we wanted to apply for groups. Let $y = (f(e_A))$ and we define $h := t_{i_B(y)} \circ f$. Then we want to show that h is a homomorphism of group schemes. To do this we consider the morphism

$$g = (A \times A \xrightarrow{(h \circ m_A) \times (i_B \circ m_B \circ (h \times h))} B \times B \xrightarrow{m_B} B) \,.$$

Now it will be enough to prove that g is constantly e_B. To do this we require the following lemma.

Lemma 2.1.7 (Rigidity)**.** *Let X, Y and Z be varieties with X complete with a K-rational point. Let $f : X \times Y \to Z$ be a morphism of varieties. If there exist y_0 in $Y(K)$ and z_0 in $Z(K)$ such that $f(X \times \{y_0\}) = \{z_0\}$, then there exists a morphism $g : Y \to Z$ such that the following diagram is commutative.*

$$\begin{tikzcd}
X \times Y \arrow[r, "f"] \arrow[d, "\pi_2"'] & Z . \\
Y \arrow[ur, dotted, "g"'] &
\end{tikzcd}$$

Where π_2 is the canonical projection.

We want to apply this to g. We have

$$g(\{e_A\} \times A) = g(A \times \{e_A\}) = \{e_B\},$$

and so g factors through both the projections to A, let say by g_1 and g_2 respectively. Let us take a point x in A. This is the image of a morphism $\mathrm{Spec}(\kappa(x)) \to A$. Since e_A is a K-rational point of A, that is a morphism $\mathrm{Spec}(K) \to A$, we have the following diagram that shows us how to see x as a point in $A \times \{e_A\}$.

$$\begin{tikzcd}
\mathrm{Spec}(\kappa(x)) \arrow[dr, dotted] \arrow[drr, bend left, "\pi"] \arrow[dddr, bend right, "x"'] & & & . \\
& A \times \{e_A\} \arrow[r] \arrow[d] & \mathrm{Spec}(K) \arrow[d, "e_A"] & \\
& A \times A \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & A \arrow[d] & \\
& A \arrow[r] & \mathrm{Spec}(K) &
\end{tikzcd}$$

Then it is not misleading to call (x, e_A) the image of $\mathrm{Spec}(\kappa(x))$ in $A \times \{e_A\}$. Now we know that $g(x, e_A) = e_B$ and that g factors through the first projection, so $g_1(x) = g(x, e_A) = e_B$. If we take now z in $A \times A$ we have $g(z) = g_1(\pi_1(z)) = e_B$ by what we have just proved. □

Remark 6. The assumption of Y complete is not necessary in the proof. We just phrased the proposition in these terms to consider all the objects in the class in which this property holds.

Corollary 2.1.8. *An abelian variety is a commutative group scheme.*

Proof. Let us consider an abelian variety A and the inversion morphism $i : A \to A$. By the proposition 2.1.6 this is a morphism of group schemes. This is equivalent to the fact that A is commutative. □

Remark 7. Rigidity lemma is a classical tool in the theory of abelian varieties and it is proved, in the case of algebraically closed field, in [10]. As announced, we cannot make this assumption (at a certain point we will discuss of Galois actions), so we slightly changed the hypothesis to be still able to prove this result, in fact we required X to have a K-rational point. This is not too restrictive since our main (and only) application of rigidity lemma is for abelian varieties and these have at least one rational point: $e_A : \mathrm{Spec}(K) \to A$.

Proof of lemma 2.1.7 (Rigidity). Let x_0 be a point in $X(K)$. We consider the morphism $(x_0, \mathrm{id}_Y) : Y \to X \times Y$, this is given by the diagram:

$$\begin{tikzcd}
Y \arrow[dd] \arrow[dr, dotted, "(x_0{,}\mathrm{id}_Y)"] \arrow[drr, bend left, "\mathrm{id}_Y"] & & \\
& X \times Y \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & Y \arrow[d] \\
\mathrm{Spec}(K) \arrow[r, "x_0"] & X \arrow[r] & \mathrm{Spec}(K)
\end{tikzcd}.$$

Now we define $g = f \circ (x_0, \mathrm{id}_Y)$. We want to check that $f = g \circ \pi_2$, from [7, Ch. 3, Prop. 3.11] it is enough to check that the two functions agree on an open dense subset of $X \times Y$. Moreover we observe that $X \times Y$ is irreducible from [17, Tag 038F] and so every open subset of it would be dense. Let U be an affine open neighborhood of z_0 in Z. Then we consider the set $W = \pi_2(f^{-1}(Z \setminus U))$, by continuity of f and completeness of X the set W is closed. Since $f(X \times \{y_0\}) = \{z_0\}$, we have $y_0 \notin W$ and so the set $V' = Y \setminus W$ is open and non-empty. We consider now a point t in $X \times Y$ lying in the open subset $V = \pi_2^{-1}(V')$. We assume now by contraddiction that t is in $f^{-1}(Z \setminus U)$, then $\pi_2(t)$ would be in W and this is not possible. So t is mapped by f to U. Moreover t can be seen as a point of $X \times \{\pi_2(t)\}$ and we claim that the morphism from $X \times \{\pi_2(t)\}$ to U can have as a possible image only a single point. So f acts the same way on every point t with the same $\pi_2(t)$. Since the map (x_0, id_Y) is a section for the second porjection, we have

$$f(t) = f \circ (x_0, \mathrm{id}_Y) \circ \pi_2(t) = g(t)\pi_2(t).$$

We are left to check the claim. We observe that $X' = X \times \{\pi_2(t)\}$ is a base change of a complete variety, then by [7, Ch. 3, Prop. 3.16] it is complete. Now, from [7, Ch. 3, Cor. 3.21] we know that $\Gamma(X', \mathcal{O}_{X'})$ is a field, let us call it k. We know that U is affine, let us say $U = \mathrm{Spec}(R)$. Now we consider

$$\mathrm{Hom}_{\mathbf{Var}_K}(X', U) \simeq \mathrm{Hom}_{\mathbf{Alg}_K}(R, \Gamma(X', \mathcal{O}_{X'})) \simeq \mathrm{Hom}_{\mathbf{Var}_K}(\mathrm{Spec}(k), U).$$

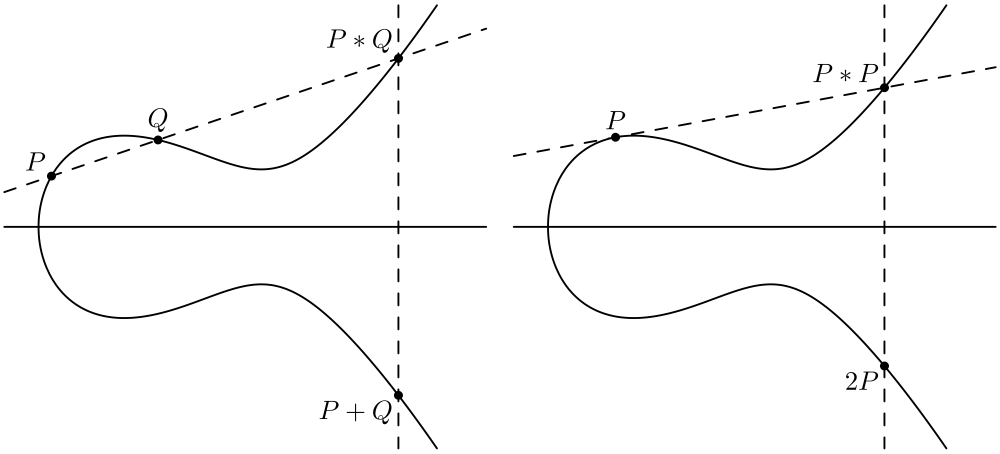
And the only morphisms in the last set are sending everything to a single point. □

This situation of rigidity does not apply for any variety let us think at the following example.
We take $X = Y = Z = \mathbb{A}^1_K$ and we consider the morphism $f : \mathbb{A}^1_K \times \mathbb{A}^1_K \to \mathbb{A}^1_K$ that is defined on closed points by $(x, y) \mapsto xy$, for $y = 0$, $z = 0$ we have the condition of the lemma. But f does not factor through the projection, for instance $f(1, 1) = 1 \neq 2 = f(2, 1)$.
We our now interested in giving an example of an abelian variety.

Example 4 (Elliptic curves)**.** An *elliptic curve* over K is a smooth curve E of genus 1 having a K-rational point O. Elliptic curves are the first example of abelian varieties. A canonical reference on the subject is [16]. Here we will briefly check that this definition actually gives an abelian variety. As in [16, III, Prop. 3.1] by Riemann-Roch theorem one can show that elliptic curves are projective plane curves described by a homogeneous polynomial of degree three. Since projective implies proper (see [7, Ch. 3, Th. 3.30]), elliptic curves are complete varieties in our sense. In [16, III §2] it is described a procedure to endow $E(K)$ with a group structure with O as the identity. Given two points P and Q in $E(K)$ if we denote by $P * Q$ the third point of intersection of the line through P and Q with E, then $P + Q$ will be given by $P + Q = O * (P * Q)$. The figure 2.1 gives an insight of this construction. From the formula deriving from this algorithm [16, III, 2.3], one sees easily that for every extension of fields $K \subset K'$ also $E(K') = E_{K'}(K')$ is a group which contains $E(K)$ as a subgroup. This is enough to show that we have a K-group scheme structure on E. In [16, III, Prop. 3.4] it is shown that there is a group structure on $E(K)$ arising from an isomorphism

$$\begin{aligned} E &\longrightarrow \mathrm{Pic}^0(E) \\ P &\longmapsto [P - O]. \end{aligned}$$

This gives exactly the same group as in the "geometrical" construction.



(a) $P \neq Q$

(b) $P = Q$

Figure 2.1

For an abelian variety A over K and an integer n coprime with the characteristic of K it is useful to understand what is the structure of its *n-torsion*, namely the group

$$A[n] := \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A(K_s))$$

where K_S denotes a separable closure of K. To do this we will give a short overview, following [18, V], on a particular kind of morphisms between abelian varieties: the isogenies.

Definition 2.1.9. Let A and B be to abelian varieties, a morphism of varieties $f : A \to B$ is called an *isogeny* if it satisfies one of the following equivalent conditions.

1. f is surjective and $\dim(A) = \dim(B)$;
2. $\ker(f)$ is a finite group scheme and $\dim(A) = \dim(B)$;
3. f is a finite, flat morphism.

The equivalence of this properties for a morphism of varieties is proved in [18, Prop. 5.9].
If we denote by $K(A) = \mathrm{Frac}(\Gamma(U, \mathcal{O}_A))$, where U is an open subset of A, the function field of A, the fact that an isogeny is surjective implies that we have a homomorphism $f^* : K(B) \to K(A)$. This translates into a finite extension of fields, we define the *degree* of an isogeny the number $[K(A) : f^*K(B)]$. We are now interested in isogenies for which this extension is separable.

Definition 2.1.10. An isogeny f is called *separable* if it satisfies one of the following equivalent conditions.

1. The field extension $K(A)/f^*K(B)$ is separable;
2. f is an étale morphism;
3. $\ker(f)$ is an étale group scheme.

See [18, Prop. 5.6].
The introduction of isogenies to study the n-torsion is justified by the following result.

Proposition 2.1.11. *Let A be an abelian variety over a field K. Let $n \neq 0$ be an integer, then $[n] : A \to A$ is an isogeny of degree $n^{2\dim(A)}$. If, moreover, n is coprime with the characteristic of K then $[n]$ is separable and the group $A[n] = \ker[n](K_s)$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(A)$.*

Proof. For the proof we refer to [18, Prop. 5.9] and [18, Cor. 5.11]. □

We are now interested in a divisibility result for the rational points on an abelian variety. In [18, Cor. 5.10], it is proved that $A(\bar{K})$ is a divisible group, unfortunately this result in not so useful for our aims. This is beacause in what follows we will be interested in a Galois action on the rational points of an abelian variety (more in general of a group scheme), this will prevent us from using anything related to the algebraic closure. But we can obtain the needed result adding a little argument on étale morphisms.

Proposition 2.1.12. *For every n coprime with the characteristic of K, the group $A(K_s)$ is n-divisible.*

Proof. The isogeny $[n]$ induces multiplication by n on $A(K_s)$. We know that $[n]$ is étale and surjective. So we are reduced to prove the following lemma. □

Lemma 2.1.13. *Let X and Y be two noetherian schemes over a field K. We denote by K_s a separable closure of K. Let $f : X \to Y$ be an étale surjective morphism of K-schemes. Then the induced map*

$$f : X(K_s) \to Y(K_s)$$

is surjective.

Proof. Let $y : \mathrm{Spec}(K_s) \to Y$ be a K_s-rational point. We consider the fiber $X_y = X \times_Y \mathrm{Spec}(K_s)$. Since f is surjective the fiber will be non-empty and by [6, Cor. 17.6.2 (c')] it has a point z such that $\kappa(z)$ is a separable extension of K_s implying that $\kappa(z) = K_s$. Then z gives a K_s-rational point on $X \times_Y \mathrm{Spec}(K_s)$ and by composition a K_s-rational point on X that is send by f to y. □

2.2 Tate modules

In this section we will show how to associate to a group scheme over K, for every prime number, a Galois module. The importance of these modules is that they encode tha arithmetic of the group scheme relatively to a given prime number. Here we will always consider K to be a field, K_s will be one of its separable closure, and G a commutative group scheme over K. Let now l be a prime number, then for every positive integer n the set

$$G[l^n] = \mathrm{Hom}(\mathbb{Z}/l^n\mathbb{Z}, G(K_s))$$

is a commutative group. Moreover, for every n, we have the following homomorphism

$$[l] : G[l^{n+1}] \longrightarrow G[l^n] \tag{2.1}$$

that sends a point to its l-multiple. It is clear that $\{G[l^n]\}_n$ is an inverse system.

Definition 2.2.1. The *Tate-l-module* of G is

$$T_l(G) := \varprojlim G[l^n]$$

We remark now that $\{\mathbb{Z}/l^n\mathbb{Z}\}_n$ is a direct system with transition maps

$$\begin{aligned} \mathbb{Z}/l^n\mathbb{Z} &\longrightarrow \mathbb{Z}/l^{n+1}\mathbb{Z} \\ 1 &\longmapsto l. \end{aligned}$$

This morphism is exactly the one inducing $[l]$ by funcoriality of $\mathrm{Hom}(-, G(K_s))$. Then we have the following equivalent description of the tate module.

$$T_l(G) = \varprojlim \mathrm{Hom}(\mathbb{Z}/l^n\mathbb{Z}, G(K_s)) = \mathrm{Hom}(\varinjlim \mathbb{Z}/l^n\mathbb{Z}, G(K_s)) = \mathrm{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, G(K_s))$$

in fact, the last direct limit comes from considering the canonical isomorphism

$$\begin{aligned} \varinjlim \mathbb{Z}/l^n\mathbb{Z} &\longrightarrow \mathbb{Q}_l/\mathbb{Z}_l \\ \mathbb{Z}/l^n\mathbb{Z} \ni x_n &\longmapsto x_n l^{-n} \end{aligned}$$

We will now provide some examples of Tate modules, considering a field K with characteristic $p \geq 0$.

Example 5. Let $G = \mathbb{G}_{a,K}$, and let $l \neq p$ be a prime number. Then for every positive integer n, the group $G[l^n]$ is exactly the l^n-torsion of K_s and so is trivial. This tells us that $T_l(\mathbb{G}_{a,K}) = 0$. On the other hand multiplication by p kills every element in $G(K_s)$, so the module $T_p(\mathbb{G}_{a,K}) = 0$ is trivial too.

Example 6. Let $G = \mathbb{G}_{m,K}$. We observe that there are no non trivial p-th roots of unity in K_s and so $T_p(\mathbb{G}_{m,K}) = 0$. We now take a prime number $l \neq p$. We assume that, for every n, we have a primitive l^n-root of unity ζ_n. Then every element of $G[l^n]$ is uniquely definied by a power of an element of ζ_n and so by an element of $\mathbb{Z}/l^n\mathbb{Z}$. If we require, moreover, the system of primitive roots to be compatible, in the sense that $\zeta_{n+1}^l = \zeta_n$, for every n, then it is clear that the Tate module $T_l(\mathbb{G}_{m,K})$ is isomorphic to $\mathbb{Z}_l$.

Example 7. Let $G = A$ be an abelian variety. Then, as a consequence of proposition 2.1.11, we have that for every prime $l \neq p$, the Tate module $T_l(A)$ is a free $\mathbb{Z}_l$-module of rank $2\dim(A)$.

In the previous examples we described some Tate modules via non-canonical isomorphisms! Even if this tells us everythiing on their structure as groups, the isomorphisms make us lose control on another structure we have on $T_l(G)$, in fact Tate modules have a galois action. The aim of the next section will be to give a first insight on the galois modules behaviour of tate modules and to study their ramification.

2.3 Tate modules as Galois representations

In this section we will show how to endow a Tate module with a non-trivial action of the absolute Galois group of the field they are defined on. Moreover we will show how, in the case of abelian varieties and of the multiplicative group, this action corresponds to a non-trivial representation of the absolute Galois group.

Let Ω/K be a Galois extension with Galois group $\mathrm{Gal}(\Omega/K)$. Every element σ in $\mathrm{Gal}(\Omega/K)$ can be seen as a K-algebras morphism $\sigma : \Omega \to \Omega$. This induces a K-morphism of schemes

$$\operatorname{Spec}\sigma : \operatorname{Spec}\Omega \longrightarrow \operatorname{Spec}\Omega.$$

If we consider a K-scheme X, then we have naturally an action of $\mathrm{Gal}(\Omega/K)$ on $X(\Omega)$. In fact, if we take an element σ in $\mathrm{Gal}(\Omega/K)$ and a point P in $X(\Omega)$, we can define the Ω-rational point $\sigma(P) := P \circ \operatorname{Spec}(\sigma)$ as in the diagram:

$$\begin{tikzcd}
\operatorname{Spec}\Omega \arrow[r, "\operatorname{Spec}\sigma"] \arrow[rr, bend right, "\sigma(P)"'] & \operatorname{Spec}\Omega \arrow[r, "P"] & X .
\end{tikzcd}$$

Our interest now is in the case $X = G$ is a group scheme over K. We know, then, that $G(\Omega)$ has a group structure. One may wonder on whether the Galois action commutes with the group scheme operations. Let P and Q be two rational points in $G(\Omega)$ and σ an element in $\mathrm{Gal}(\Omega/K)$. We consider the following diagram.

$$\begin{tikzcd}
\operatorname{Spec}\Omega \arrow[dr, "\operatorname{Spec}\sigma"] \arrow[rrrrdd, bend left, "\sigma(Q)"] \arrow[ddddrr, bend right, "\sigma(P)"'] & & & & . \\
& \operatorname{Spec}\Omega \arrow[dr, "{(P,Q)}"] \arrow[rrrd, bend left, "Q"] \arrow[dddr, bend right, "P"'] & & & \\
& & G \times_K G \arrow[rr] \arrow[dr, "m"] \arrow[dd] & & G \arrow[dd] \\
& & & G & \\
& & G \arrow[rr] & & \operatorname{Spec} K
\end{tikzcd}$$

We know that

$$\sigma(P * Q) = m \circ (P,Q) \circ \operatorname{Spec}\sigma,$$

while on the other hand

$$(\sigma(P) * \sigma(Q)) = m \circ (\sigma(P), \sigma(Q)).$$

As we can see in the diagram above, the universal property of the fiber product tells us that $(P,Q) \circ \operatorname{Spec}\sigma = (\sigma(P), \sigma(Q))$, and so we can conclude that the Galois action commutes with the group operation on $G(\Omega)$.
We consider now the case in which G is a commutative group scheme over K. Then if K_s is a separable closure of K, we have an action of $\mathrm{Gal}(K_s/K)$ on $G(K_s)$. The fact that the action commutes with the group operation, immediately tells us that the Galois action can be extended to $G[m]$. Since, moreover, the Galois action commutes with taking integer multiples of points in $G(K_s)$, we have a Galois action also on $T_l(G)$, for any prime number l. This means that we have a homomorphism of groups

$$\rho : \mathrm{Gal}(K_s/K) \longrightarrow \mathrm{Aut}(T_l(G)).$$

An important case will be when we consider $G = A$ to be an abelian variety over K, and l a prime number not dividing the characteristic of K. As seen in the example 7, the l-Tate module $T_l(A)$ is a free $\mathbb{Z}_l$-module. Multiplication by an element of $\mathbb{Z}_l$ is just a compatible componentwise multiplication by integer numbers, this implies that the Galois action and the $\mathbb{Z}_l$-module structure on $T_l(A)$ are compatible. This amounts to say that the homomorphism of groups ρ is actually a homomorphism

$$\rho : \mathrm{Gal}(K_s/K) \longrightarrow \mathrm{GL}_{2\dim(A)}(\mathbb{Z}_l).$$

This is an example of what is called a *Galois representation*. Now we will provide another example, a Galois representation associated to the multiplicative group, in this case we will assume the base field to be $K = \mathbb{Q}_p$, for a certain prime number p, to do concrete computations.

Example 8. We will consider the Tate module $T_l(\mathbb{G}_{m,K})$ as in the example 6. We assume the field K to be $\mathbb{Q}_p$ for a certain prime number p, and then K_s will be

$\bar{\mathbb{Q}}_p$ an algebraic closure of $\mathbb{Q}_p$. Let l be a prime number. We assume we fixed a compatible sequence of primitive l^n-th roots of unity as in the example 6. Then for every n, an element σ in the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts sending each ζ_n to another primitive l^n-th root, in other terms

$$\sigma(\zeta_n) = (\zeta_n)^{a_{\sigma,n}}$$

where $a_{\sigma,n}$ is coprime with l and well defined modulo l^n, that is we can consider $a_{\sigma,n}$ as an element of $(\mathbb{Z}/l^n\mathbb{Z})^\times$. The compatibility in the choice of the ζ_n's tells us that then, for each n,

$$l a_{\sigma,n+1} \equiv a_{\sigma,n} \pmod{l^n}.$$

This means that the action of σ is univocally determined by an element in $(\mathbb{Z}_l)^\times$. Resuming, we have a surjective homomorphism

$$\begin{aligned} \rho : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) &\longrightarrow (\mathbb{Z}_l)^\times \simeq \mathrm{Aut}(T_l(\mathbb{G}_{m,\mathbb{Q}_p})) \\ \sigma &\longmapsto (a_{\sigma,1}, a_{\sigma,2}, \ldots, a_{\sigma,n}, \ldots). \end{aligned}$$

If we assume K to be a field with a discrete valuation v, it will be meaningful to ask whether a Tate module $T_l(G)$ is unramified at v looking at the action of the inertia group $I(\bar{v})$.

Definition 2.3.1. We say that $T_l(G)$ is unramified at v if $\rho(I(\bar{v})) = \{1\}$.

When $G = A$ is an abelian variety, is not easy to discuss the ramification of the associated Tate modules by direct computation. What we will do in the last chapter is to show a criterion that relates this to another property of the abelian varieties: good reduction.

Coming back to example 8, we are able to compute for which prime numbers l the Tate module $T_l(\mathbb{G}_{m,K})$ is unramified over p.

We first consider the case $l \neq p$. We will show that for each n the root ζ_n is contained in an unramified extension, this will prove, thanks to proposition 1.2.10, that the inertia group I acts trivially on $T_l(\mathbb{G}_{m,\mathbb{Q}_p})$. We claim that the maximal unramified extension of $\mathbb{Q}_p$ is given by all the m-th roots of unity, with $(m,p) = 1$ and so $T_l(\mathbb{G}_{m,\mathbb{Q}_p})$ is unramified. Similarly, one sees that $T_p(\mathbb{G}_{m,\mathbb{Q}_p})$ is ramified.

To prove our claim we observe that there is a one to one correspondence between unramified finite extensions of $\mathbb{Q}_p$ and finite extensions of $\mathbb{F}_p$ (this is an easy check using Hensel's lemma). For every n the field $\mathbb{F}_p$ has a unique finite extension of degree n, given by the splitting field of the polynomial $x^{p^n} - x$. The corresponding field extension of $\mathbb{Q}_p$ will be the splitting field of $x^{p^n} - x$ over $\mathbb{Q}_p$, that is the cyclotomic extension obtained adding the $(p^n - 1)$-th roots of unity. Taking the compositum of all those extensions, we observe that the maximal unramified extension of $\mathbb{Q}_p$ is obtained adding all the $(p^n - 1)$-th roots of unity for every n. If now m is an integer coprime with p, we have

$$p^{\varphi(m)} \equiv 1 \pmod{m}$$

this shows that every m-th root of unity is a $(p^{\varphi(m)} - 1)$-th root of unity, proving our claim. When we refer to the module $\mathbb{Z}_l$ with the Galois action just described, we use the notation $\mathbb{Z}_l(1)$.

2.4 Abelian schemes

Let us consider an elliptic curve over $\mathbb{Q}_{|}$ described by the Weierstrass equation

$$E : y^2 = x^3 + ax + b$$

with a and b in $\mathbb{Z}_p$. What happens if we look at the equation modulo p? We will obtain a curve $\tilde{E}$ over $\mathbb{F}_p$ described by

$$\tilde{E} : y^2 = x^3 + \bar{a}x + \bar{b}.$$

If the curve we obtained after reduction is non-singular, then it is still an elliptic curve, this will allow us to study the arithmetic of $\tilde{E}$ on a finite field to recover information on the original curve E. For motivations and a complete and detailed discussion on the subject we suggest to look at [16, VII]. This situation, the non-singularity of $\tilde{E}$, has the right to be addressed as "good". In fact we say that an elliptic curve E over $\mathbb{Q}_p$ has *good reduction* at p if there is an equation for E with coefficients in $\mathbb{Z}_p$ such that when reduced modulo p describes an elliptic curve over $\mathbb{F}_p$. To have good reduction we require an equation over $\mathbb{Z}_p$ (a scheme E_p over $\mathrm{Spec}(\mathbb{Z}_p)$?), that describes E over $\mathbb{Q}_p$ (the generic fiber $E_p \times \mathbb{Q}_p \simeq E$?) and such that its reduction is an elliptic curve (the special fiber $E_p \times \mathbb{F}_p$ is an elliptic curve?). From this observation is reasonable to think of good reduction as the existence of a "family" of elliptic curves parametrized by the points of $\mathrm{Spec}(\mathbb{Z}_p)$.
We want an object to describe this situation for abelian varieties, we will introduce abelian schemes, these are schemes over a base S, that in a certain sense are parametrized collections of abelian varieties.
In this context we will use definitions and properties from [9, Ch. 6].

Definition 2.4.1. A group scheme X over S is called an *abelian scheme* if it is smooth, proper and with connected geometrically connected fibers.

Now we want to check that with this definition a fiber $X_s = X \times_S \kappa(s)$ of an abelian scheme X is an abelian variety over $\kappa(s)$. First of all, as we observed in the first section, X_s naturally inherits a structure of group scheme. Moreover by [7, Ch. 3, Prop. 3.16] the base change of a proper morphism is still proper, so X_s will be complete and of finite type. A point in which X_s (or any of its base change) is not reduced would contraddict smoothness, so X_s is geometrically reduced. Finally assume by contraddiction that a certain base change X_s' of X_s is reducible. Since X_s is geometrically connected, X_s' has two irreducible components intersecting in a point. The existence of such a point contraddicts smoothness.
In [9, Ch. 6, §1] it is shown that an equivalent statement of rigidity lemma for abelian schemes is holding. Starting from this it is possible to reproduce what we did in the section 2, and obtain the following results.

Corollary 2.4.2. *Let X be an abelian scheme over S and G a group scheme over S. Then every morphism of schemese $f : X \to G$ is the composition of a translation and a homomorphism of group schemes.*

Corollary 2.4.3. *An abelian scheme is a commutative group scheme*

After we defined abelian schemes we come back to the problem of reduction. We fix a base field K with a discrete valuation v. As usual we will keep the notation as in section 1.2.

Definition 2.4.4. Let A be an abelian variety over K. We say that A has good reduction at v if there exists an abelian scheme A_v over $\mathcal{O}_v$, such that

$$A \simeq A_v \times_{\mathcal{O}_v} K$$

For elliptic curves we can always transform the equation to obtain coefficients in $\mathcal{O}_v$ and then check what happens modulo $\mathfrak{m}_v$, in a certain sense we always have a candidate to check good reduction. For abelian varieties the lack of an equation, in general, prevent us to aplly such an argument. What we are going to use are Néron models.

2.5 Néron models

When dealing with Néron models one usally works over a base scheme S that is a Dedekind scheme and K its field of rational functions, as in [1]). A *Dedekind scheme* is a noetherian normal scheme of dimension ≤ 1. For our purposes we assume K to be a field with a discrete valuation v and the base scheme to be $S = \mathrm{Spec}(\mathcal{O}_v)$ since we do not need so much generality. For valuation theory we will follow the notation we used in chapter 1.2.

Definition 2.5.1. Let X be a separated, smooth scheme of finite type over K. A *model* for X relative to v is an $\mathcal{O}_v$-scheme X_v such that

$$X \simeq X_v \times_{\mathcal{O}_v} \mathrm{Spec}(K).$$

Néron models are a class of models satisfying a particular universal property.

Definition 2.5.2. Let X be a separated, smooth scheme of finite type over K. A *Néron model* for X relative to v is a separated, smooth model for X of finite type satisfying the *Néron mapping property.* That is for every smooth $\mathcal{O}_v$-scheme Y, and for every K-morphism $f : Y_K \to X$, there exist a unique $\mathcal{O}_v$-morphism $f_v : Y \to X_v$ that extends f (meaning that the base change of f_v by K is f).
In other terms the functor from the category of smooth $\mathcal{O}_v$-schemes to **Set** given by

$$Y \longmapsto \mathrm{Hom}_K(Y_K, X)$$

is representable by X_v.

An immediate consequence of the definition is that a Néron model for a given scheme is unique up to a unique isomorphism. Another straightforward application tells us that

$$X(K) = X_v(\mathcal{O}_v).$$

What we are interested in is the behaviour of Néron models with respect to field extensions. Following the same notation as in 1.2 we consider a finite extension K' over K with a discrete valuation v' extending v. Then we have the following property on N'eron models.

Proposition 2.5.3. *Let X_v be a Néron model relative to v for a smooth, separated K-scheme of finite type X_K. If K'/K is a separable and unramified extension of discrete valuation fields, the $\mathcal{O}_{v'}$-scheme $X_{v'} = X_v \times_{\mathcal{O}_v} \operatorname{Spec}(\mathcal{O}_{v'})$ is a Néron model for $X'_K = X \times_K \operatorname{Spec}(K')$ relative to v'.*

Proof. Firstly from stability by base change we obtain that $X_{v'}$ is separated, smooth and of finite type. We want to remark that, since K'/K is separable and unramified, the morphism $\operatorname{Spec}(\mathcal{O}_{v'}) \to \operatorname{Spec}(\mathcal{O}_v)$ is étale. Our aim is to prove now the Néron mapping property for $X_{v'}$. We take a smooth $\mathcal{O}_{v'}$-scheme Y and a morphism $Y_{K'} \to X_{K'}$. By composition with the projection, this induces a morphism $Y_{K'} \to X$. Moreover Y is smooth over $\mathcal{O}_v$, in fact the composition of a smooth morphism with an étale morphism is smooth (see [7, Ch. 4, Cor. 3.24; Prop. 3.38]). So by Néron mapping property of X_v we have a unique morphism $Y \to X_v$, now by base change we obtain a morphism $Y \to X_{v'}$. By construction this morphism is unique. □

We have that for abelian varieties there exist a Néron model.

Proposition 2.5.4. *Let A be an abelian variety over K. Then there exist a Néron model A_v for A relative to v.*

Proof. See [1, Ch.1 , §3, Cor. 2]. □

The first thing one notices is that Néron mapping property trasports the group scheme structure from A to A_v. This apply to every group scheme in general.

Proposition 2.5.5. *Let X be a group scheme, separated, smooth and of finite type over K. Let X_v be a Néron model for X. Then X_v is naturally a group scheme.*

Proof. This is essentially Néron mapping property. The morphism $m : X \times_K X \to X$ is lifted to a morphism $X_v \times_{\mathcal{O}_v} X_v \to X_v$. The same argument applies for the identity section and the inversion morphism. The fact that the required diagrams commute is due to the unicity of such liftings. □

Néron models for abelian varieties can be used to check their good reduction. If an abelian variety A has good reduction at v, the abelian scheme A_v whose generic fiber is A is a Néron model for A. This is shown in [1, Ch. 1, §2, Prop. 8]. Now our interst is in understanding when a Néron model for A tells us that it has good reduction.

Proposition 2.5.6. *Let A be an abelian variety over K. Let A_v be a Néron model for A relative to v. Then if A_v is proper A has good reduction at v.*

Proof. Since A_v is a model for A, it is enough to show that A_v is an abelian scheme. We already know that A_v is proper and smooth, what is left to prove is that the fibers are geometrically connected. We know that there are two fibers, the generic one which is an abelian variety hence geometrically connected, and the special one. A straightforward use of the result in [4, Prop. 5.5.1] tells us that the special fiber $A_v \times_{\mathcal{O}_v} k$, being proper, is connected up to base change with a complete extension of the base field K. Applying this argument to every base change we obtain the geometrically connectedness. □

Chapter 3

The Néron-Ogg-Shafarevich Criterion

3.1 Decomposition of group schemes and their torsion

Remark 8. Here for the first time we will talk about exact sequences of group schemes. To add some rigor to this we should be able to take kernels and cokernels (more in general quotients) in the category of group schemes. While the definition of kernel comes pretty natural (either functorially, either with a fiber product) cokernels are more difficult to handle. The good environment to take in account is the category of abelian sheaves on fppf topologies. Group schemes will form a full subcategory of this one, cokernels (and kernels) will be intended in this category. Here no further detail will be given about this question, the subject is covered enough in [18, IV].

In this section we will collect some decomposition results for group schemes. Later we will compute the torsion for the objects appearing in these decompositions. Finally we summarize all the section in one lemma that will be fundamental in the proof of the Néron-Ogg-Shafarevich criterion.
Now we are providing a tool that will be useful throughout this section, to prove it one should use étale cohomology, a subject we are not going to treat, that is why our proof will be just a sketch. We will refer to [8] for the notation and for a more detailed argument.

Lemma 3.1.1. *Let*

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

be a short exact sequence of commutative group schemes over a separably closed field $K = K_s$. We assume moreover G' to be quasi-projective (for example affine) and smooth. Then

$$0 \longrightarrow G'(K) \longrightarrow G(K) \longrightarrow G''(K) \longrightarrow 0$$

is a short exact sequence of groups.

Proof. As we noticed in example 3, for every K-group schemes H we have

$$\mathrm{Hom}_{\mathbf{Sch}_K}(\mathrm{Spec}(K), H) = \mathrm{Hom}_{\mathbf{GrpSch}_K}(\mathbb{Z}_{\mathrm{Spec}(K)}, H) = \mathrm{Hom}_{\mathbf{fl}_K}(\mathbb{Z}_{\mathrm{Spec}(K)}, H),$$

where the last term are the homomorphism in the fppf sheaves category. So what we want to show is that $\mathrm{Ext}^1_{\mathbf{fl}_K}(\mathbb{Z}_{\mathrm{Spec}(K)}, G') = 0$. That is, in the notation of [8], $\mathrm{H}^1_{\mathbf{fl}_K}(\mathrm{Spec}(K), G') = 0$. Since G' is smooth and quasi-projective, we can apply the étale-flat comparison theorem ([8, III, Th. 3.9]). Hence we have

$$\mathrm{H}^1_{\mathbf{fl}_K}(\mathrm{Spec}(K), G') \simeq \mathrm{H}^1_{\mathbf{\acute{e}t}_K}(\mathrm{Spec}(K), G').$$

Now a Čech cohomology argument shows that $\mathrm{H}^1_{\mathbf{\acute{e}t}_K}(\mathrm{Spec}(K), G') = 0$. □

Definition 3.1.2. Let T be a group scheme over S. For every point s in S let $\kappa(s)$ be a separable closure of its residue field. We say that T is a *torus* if for every point s in S

$$T \times_S \mathrm{Spec}(\kappa(s)) \simeq \mathbb{T}^{n(s)}_{m,\kappa(s)}$$

where the function $n : S \to \mathbb{N}$ is locally constant.

Definition 3.1.3. Let U be a group scheme over S. We say that U is a *unipotent group* if there exists a finite chain of normal subgroup schemes

$$1 = U_0 \subset U_1 \subset \cdots \subset U_{n-1} \subset U_n = U$$

such that U_{i+1}/U_i is isomorphic to $\mathbb{G}_{a,S}$ fore every $i = 0, 1, ..., n$.

Even if we defined these group schemes over any base S, for the rest of the section we are only considering group schemes over a perfect field K. Now we question their m-divisibility and compute their m-torsion when m is an integer coprime with the characteristic of the field K. The reader should be aware that we are using the notation $G[m] = \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, G(K_s)$.

Lemma 3.1.4. *Let T be a torus over K. Let m be an integer coprime with* $\mathrm{char}(K)$*. Then the group $T(K_s)$ is m-divisible and $T[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank* $\dim(T)$*.*

Proof. As T is defined over $\mathrm{Spec}(K)$, and this topologically is just a point, by definition T_{K_s} is isomorphic to $\mathbb{G}^n_{m,K_s}$. Since the dimension of $\mathbb{G}^n_{m,K_s}$ is n, we have $\dim(T) = \dim(T_{K_s}) = n$. Now

$$T(K_s) = T_{K_s}(K_s) = \mathbb{G}^n_{m,K_s}(K_s) = (K_s^\times)^n.$$

Knowing that m is coprime with $\mathrm{char}(K)$, the polynomials $X^m - \alpha$, for $\alpha \in K_s$, are separable over K_s. Hence they have m distinguished roots in K_s. This shows that $T(K_s)$ is m-divisible. The same argument for $\alpha = 1$ shows that $T[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $n = \dim(T)$. □

Lemma 3.1.5. *Let U be a commutative unipotent group over K. Let m be an integer coprime with* $\mathrm{char}(K)$*. Then the group $U(K_s)$ is m-divisible and it does not have elements of order m.*

Proof. From the definition we have a chain of normal subgroup schemes

$$0 = U_0 \subset U_1 \subset \cdots \subset U_n = G.$$

Such that for every index i we have a short exact sequence

$$0 \longrightarrow U_i \longrightarrow U_{i+1} \longrightarrow \mathbb{G}_{a,K} \longrightarrow 0.$$

Then we apply lemma 3.1.1 and denoting $W_i = U_i(K_s)$, for every index i, we obtain a short exact sequence

$$0 \longrightarrow W_i \longrightarrow W_{i+1} \longrightarrow K_s \longrightarrow 0.$$

We will now prove our lemma by finite induction on i.
For $i = 0$ we have that

$$0 \longrightarrow W_0 \longrightarrow W_1 \longrightarrow K_s \longrightarrow 0$$

is exact, then W_1 is isomorphic to K_s and so it is m-divisible and m-torsion free. What is left to prove is the inductive step. Assume that W_i is m-divisible and m-torsion free. We have the following diagram

$$\begin{tikzcd}
0 \arrow[r] & W_i \arrow[r] \arrow[d, "m_i"] & W_{i+1} \arrow[r] \arrow[d, "m_{i+1}"] & K_s \arrow[r] \arrow[d, "m"] & 0 \\
0 \arrow[r] & W_i \arrow[r] & W_{i+1} \arrow[r] & K_s \arrow[r] & 0.
\end{tikzcd}$$

where the rows are exact, the vertical maps are giving the m-multiple and the squares are commutative. This allows us to use snake lemma. Then we have a long exact sequence

$$0 \longrightarrow \ker m_i \longrightarrow \ker m_{i+1} \longrightarrow \ker m \xrightarrow{d}$$
$$\xrightarrow{d} \operatorname{coker} m_i \longrightarrow \operatorname{coker} m_{i+1} \longrightarrow \operatorname{coker} m \longrightarrow 0.$$

Since K_s is m-divisible and m-torsion free, $\ker m = 0$ and $\operatorname{coker} m = 0$. Since, by inductive hypothesis, W_i is m-divisible and m-torsion free $\ker m_i = 0$ and $\operatorname{coker} m_i = 0$. In the long exact sequence this implies that $\ker m_{i+1} = 0$ and $\operatorname{coker} m_{i+1} = 0$, that is $Wi + 1$ is m-divisible and m-torsion free. □

The following are the two decomposition results we are going to use.

Theorem 3.1.6 (Chevalley)**.** *Let K be a perfect field. Let G be a group variety over K. Then there is an exact sequence*

$$1 \longrightarrow H \longrightarrow G \longrightarrow B \longrightarrow 1 \tag{3.1}$$

where B is an abelian variety, and H is an affine group variety.

Proof. For the proof we refer to [2]. □

Theorem 3.1.7. *Let K be a perfect field. Let H be a commutative affine group variety over K. Then H has a decomposition $H = T \times_K U$ where T is a torus and U is a unipotent group.*

Proof. See [19, Th. 9.5]. □

Finally we will put together all the results seen in this section.

Lemma 3.1.8. *Let G be a commutative group variety over a perfect field K. Let H be an affine commutative group variety and let B be an abelian variety such that*

$$1 \longrightarrow H \longrightarrow G \longrightarrow B \longrightarrow 1 \tag{3.2}$$

is a short exact sequence. Let T and U be respectively a torus and a unipotent group such that $H = T \times_K U$. Then for every integer m coprime with the characteristic of K we have that $G[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $\dim(T) + 2\dim(B)$.

Proof. From lemma 3.1.1 the functor $\mathrm{Hom}(\mathrm{Spec}(\bar{K}), -)$ is exact. So, applying this to (3.2), we obtain that

$$0 \longrightarrow H(\bar{K}) \longrightarrow G(\bar{K}) \longrightarrow B(\bar{K}) \longrightarrow 0$$

is exact. We now apply the functor $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, -)$, this gives us the exact sequence

$$0 \longrightarrow H[m] \longrightarrow G[m] \longrightarrow B[m] \longrightarrow \mathrm{Ext}^1(\mathbb{Z}/m\mathbb{Z}, H(\bar{K})).$$

Since $H(\bar{K}) = T(\bar{K}) \times U(\bar{K})$ is m-divisible, since it is the product of two m-divisible groups, then $\mathrm{Ext}^1(\mathbb{Z}/m\mathbb{Z}, H(\bar{K}))$ is trivial. To prove this we consider an m-divisible group M. From $[m] : M \twoheadrightarrow M$ we obtain a long exact sequence applying the functor $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, -)$ and its derived functor $\mathrm{Ext}^1(\mathbb{Z}/m\mathbb{Z}, -)$. At this point is just a matter of computing the homomorphisms between the extension groups we obtained. Then we have a short exact sequence

$$0 \longrightarrow H[m] \longrightarrow G[m] \longrightarrow B[m] \longrightarrow 0. \tag{3.3}$$

Now $H[m] = T[m] \times U[m]$ so by lemmas 3.1.4 and 3.1.5 we deduce that $H[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $\dim(T)$. By proposition 2.1.11 we know that $B[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2\dim(B)$, and so by exactness of the sequence (3.3) we have the stated result. □

3.2 The proof of the criterion

In this section we will show the *Néron-Ogg-Shafarevich criterion* for good reduction of abelian varieties. It explains how the good reduction of an abelian variety A at a discrete valuation v, is related to the non-ramification of some torsion group. Here we will keep the notation we used for ramification theory in section 1.2 and the terminology of section 2.4 for good reduction and Néron models.

Theorem 3.2.1. *Let K be a field with a discrete valutation v such that its residue field k is perfect. Let A be an abelian variety over K and l a prime number different from the characteristic of k. Then the following are equivalent:*

(a) A has good reduction at v;

(b) $A[m]$ is unramified at v for every integer m coprime to $\mathrm{char}(k)$*;*

(c) $A[m]$ is unramified at v for infinitely many integers m coprime to $\mathrm{char}(k)$*;*

(d) $T_l(A)$ is unramified at v.

Proof. Since (d) is equivalent to the fact that A_{l^n} is unramified for every positive integer n, we have that (b) ⇒ (d) ⇒ (c). For every integer m coprime with $\mathrm{char}(k)$ we define $A[m]^I$ to be the set of elements of $A[m]$ invariant by the action of the inertia group $I = I(\bar{v})$. Our aim now is to prove that if A has good reduction at v, then $A[m]$ is equal to $A[m]^I$. In order to do that we denote by A_v the Néron model of A relative to v (we have seen that it exists in section 2.4), we recall that this is a commutative smooth group scheme of finite type over O_v. We denote with $\tilde{A} = A_v \times_{O_v} k$ the special fiber of A_v, this is a commutative group scheme over k, moreover $\tilde{A}$ is smooth, separated and of finite type. We want to remark that $\tilde{A}$ do not need to be connected. We introduced this object because of the following result.

Lemma 3.2.2. *There is an isomorphism between $A[m]^I$ and $\tilde{A}[m]$.*

Proof of 3.2.2. Let L be the fixed field of I, that is the maximal unramified extension of K. Let $\mathcal{O}_L$ be its ring of $\bar{v}$-integers. We recall that lemma 1.2.12 shows that $\mathcal{O}_L$ is an henselian ring. Then its residue field is $\bar{k}$. We want to show now that $A_v(O_L)$ is equal to $A(L)$: this essentially come from the properties of Néron models. We consider a morphism $\mathrm{Spec}(L) \to A$, since A is of finite type, this morphism factors through $\mathrm{Spec}(K') \to A$, with K' finite over K. Moreover K' is unramfied over K and so, denoting $\mathcal{O}_{K'} = K' \cap \mathcal{O}_{\bar{v}}$, we have that $\mathrm{Spec}(\mathcal{O}_{K'})$ is étale over $\mathrm{Spec}(\mathcal{O}_v)$. By the fact that Néron models commute with étale base change, we obtain a unique morphism $\mathrm{Spec}(\mathcal{O}_{K'}) \to A_v$ extending it. Composing with the map $\mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_{K'})$ we finally obtain a morphism $\mathrm{Spec}(\mathcal{O}_L) \to A_v$. Considering the unicity of the lift, we obtain $A(L) = A_v(\mathcal{O}_L)$. Now the reduction $O_L \to \bar{k}$ induces a homomorphism of groups

$$r : A(L) = A_v(O_L) \longrightarrow \tilde{A}(\bar{k}).$$

Then r is surjective because A_v is smooth and O_L is henselian. In fact, reducing ourselves to the affine case, this is exactly multivariate hensel lemma, with the smoothness condition ensuring us that we are in the condition to apply it. Moreover multiplication by m is an étale endomorphism of A_v, and since, again, $\mathcal{O}_L$ is henselian, the kernel of r is uniquely divisible by m. Applying the left-exact funtor $Hom(\mathbb{Z}/m\mathbb{Z}, -)$ to

$$0 \longrightarrow \ker(r) \longrightarrow A(L) \longrightarrow \tilde{A}(\bar{k})$$

we show that r induces an isomorphism

$$A^I[m] = \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, A(L)) \longrightarrow \tilde{A}[m] = \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \tilde{A}(\bar{k})).$$

□

If now we assume tha A has good reduction at v we have that $\tilde{A}$ is an abelian variety (it is the fiber of an abelian scheme), this implies that $\tilde{A}[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2\dim(\tilde{A})$. Since $\dim(A) = \dim(\tilde{A})$ we have an isomorphism between $A[m]$ and $\tilde{A}[m]$, then the lemma implies that $A[m]^I{=}A[m]$, and so (a) ⇒ (b).
Now we prove (c)⇒(a). We will write $\tilde{A}^0$ to denote the connected component of $\tilde{A}$ containing the identity. We observe now that since $\tilde{A}$ has finitely many connected

components (it is of finite type), the index of $\tilde{A}^0(\bar{k})$ in $\tilde{A}(\bar{k})$ is finite, we call this number c. To see this we take two points x and y in the same connected component $\tilde{A}'$, then the image of the translation $t_{-y} : \tilde{A}' \to \tilde{A}$ contains the identity e and $x-y$. Moreover the translation is continuous and so its image should be connected, then $x-y$ is in $\tilde{A}^0(\bar{k})$.
We now assume that (c) holds, we want to prove that A has good reduction at v. By hypothesis, there exists an arbitrarly large integer m such that $A[m] = A[m]^I$. We take $m \geq c$ and we consider the exact sequence

$$0 \longrightarrow \tilde{A}^0[m] \longrightarrow \tilde{A}[m] \longrightarrow \frac{\tilde{A}[m]}{\tilde{A}^0[m]} \longrightarrow 0. \tag{3.4}$$

Now, from the hypothesis and form lemma 3.2.2 we have $A[m] = A[m]^I \simeq \tilde{A}[m]$, so $\tilde{A}[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2\dim(A)$, from lemma 3.1.8 we have that $\tilde{A}^0[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $\dim(T) + 2\dim(B)$. Since $\tilde{A}[m]/\tilde{A}^0[m]$ has less than m elements, its rank as a $\mathbb{Z}/m\mathbb{Z}$-module is 0. Then (3.4) tells us that

$$\dim(T) + 2\dim(B) \geq 2\dim(A). \tag{3.5}$$

Now Since $\dim(\tilde{A}) = \dim(\tilde{A}_0)$ beacuse translations are isomorphisms of schemes and $\dim(\tilde{A}) = \dim(A)$ beacuse base change witha field preserves dimension. Finally $\dim(\tilde{A}_0) = \dim(U) + \dim(T) + \dim(B)$ (this comes from the decopositions), and so $\dim(A) = \dim(U) + \dim(T) + \dim(B)$. Adding this to (3.5) we get $U = T = 0$. So $\tilde{A}^0$ is an abelian variety, hence proper, implying $\tilde{A}$ is proper (see [7, Ch. 3, Lemma 3.15]). As we showed in proposition 2.5.6, we conclude if we show that A_v is proper. Since geometrically connectedness is ascending and properness is descending (see [5, Prop. 2.7.1]), we can assume O_v complete. Then by [4, Cor. 5.5.2], there exist two open disjoint subschemes Z and Z' of A_v sucht that, $A_v = Z \cup Z'$, where Z is proper and $\tilde{A} \subset Z$. Since A is connected, $Z' = \varnothing$ and so $A_v = Z$ is proper. □

Bibliography

[1] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)].* Springer-Verlag, Berlin, 1990.

[2] Brian Conrad. A modern proof of Chevalley's theorem on algebraic groups. *J. Ramanujan Math. Soc.*, 17(1):1–18, 2002.

[3] A. Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[4] A. Grothendieck. Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I. *Inst. Hautes Études Sci. Publ. Math.*, (11):167, 1961.

[5] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. *Inst. Hautes Études Sci. Publ. Math.*, (24):231, 1965.

[6] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[7] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[8] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[9] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)].* Springer-Verlag, Berlin, third edition, 1994.

[10] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics.* Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[11] André Néron. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ.Math. No.*, 21:128, 1964.

[12] A. P. Ogg. Elliptic curves and wild ramification. *Amer. J. Math.*, 89:1–21, 1967.

[13] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, second edition, 2010.

[14] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[15] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[16] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[17] The Stacks Project Authors. Stacks project. `http://stacks.math.columbia.edu`, 2014.

[18] Gerard van der Geer and Ben Moonen. "Abelian varieties". Available at http://staff.science.uva.nl/ bmoonen/boek/BookAV.html.

[19] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979.